I

107TH CONGRESS
2D SESSION

H. R. 3844

To strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.

IN THE HOUSE OF REPRESENTATIVES

MARCH 5, 2002

Mr. TOM DAVIS of Virginia (for himself and Mr. HORN) introduced the following bill; which was referred to the Committee on Government Reform, and in addition to the Committee on Science, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. INFORMATION SECURITY.

(a) SHORT TITLE.—The amendments made by this section may be cited as the ''Federal Information Security Management Act of 2002''.

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended to read as follows:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3531. Purposes

''The purposes of this subchapter are to—

''(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

''(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems; and

''(4) provide a mechanism for improved oversight of Federal agency information security programs.

"§ 3532. Definitions

''(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter—

''(1) the term 'information security' means protecting information and information systems from unauthorized use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

''(B) confidentiality, which means preserving an appropriate level of information secrecy; and

''(C) availability, which means ensuring timely and reliable access to and use of information;

''(2) the term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(A) the function, operation, or use of which—

''(i) involves intelligence activities;

''(ii) involves cryptologic activities related to national security;

''(iii) involves command and control of military forces;

''(iv) involves equipment that is an integral part of a weapon or weapons system; or

''(v) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

''(B) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

''(3) the term 'information technology' has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

"§ 3533. Authority and functions of the Director

''(a) The Director shall oversee agency information security policies and practices, including—

''(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through the promulgation of standards and guidelines under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

''(2) requiring agencies, consistent with the standards and guidelines promulgated under such section 5131 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of—

''(A) information collected or maintained by or on behalf of an agency; or

''(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) to enforce accountability for compliance with such requirements;

''(5) coordinating information security policies and procedures with related information resources management policies and procedures;

''(6) overseeing the development and operation of the Federal information security incident center established under section 3536; and

''(7) reporting to Congress on agency compliance with the requirements of this subchapter, including—

''(A) a summary of the findings of evaluations required by section 3535;

''(B) significant deficiencies in agency information security practices; and

''(C) planned remedial action to address such deficiencies.

''(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

''§ 3534. Federal agency responsibilities

''(a) The head of each agency shall—

''(1) be responsible for—

''(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of the agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

''(i) information security standards and guidelines promulgated by the Director under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); and

''(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

''(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

''(A) assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) for information security classifications and related requirements;

''(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

''(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

''(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

''(A) designating a senior agency information security officer who shall—

''(i) carry out the Chief Information Officer's responsibilities under this section;

''(ii) possess professional qualifications, including training and experience,

required to administer the functions described under this section;

"(iii) have information security duties as that official's primary duty; and

"(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

"(B) developing and maintaining an agencywide information security program as required by subsection (b);

"(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3533 of this title, and section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(E) assisting senior agency officials concerning their responsibilities under subparagraph (2);

"(4) ensure that the agency has trained personnel sufficient to assist the agency in complying

with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

''(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

''(b) Each agency shall develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

''(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

''(2) policies and procedures that—

''(A) are based on the risk assessments required by subparagraph (1);

''(B) cost-effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

"(D) ensure compliance with—

"(i) the requirements of this subchapter;

"(ii) policies and procedures as may be prescribed by the Director, including information security standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); and

"(iii) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

"(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

"(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

"(A) information security risks associated with their activities; and

"(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

"(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually;

"(6) a process for ensuring remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) procedures for detecting, reporting, and responding to security incidents, consistent with guidance issued under section 3536, including—

"(A) mitigating risks associated with such incidents before substantial damage is done;

"(B) notifying and consulting with the Federal information security incident center established under section 3536; and

"(C) notifying and consulting with, as appropriate—

"(i) law enforcement agencies and relevant Offices of Inspector General;

''(ii) an office designated by the President for any incident involving a national security system; and

''(iii) any other agency or office, in accordance with law or as directed by the President; and

''(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

''(c) Each agency shall—

''(1) report annually to the Director and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, including compliance with the requirements of this subchapter;

''(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

''(A) annual agency budgets;

''(B) information resources management under subchapter 1 of this chapter;

''(C) information technology management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

"(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

"(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

"(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

"(G) internal accounting and administrative controls under section 3512 of title 31, United States Code, (known as the 'Federal Managers Financial Integrity Act'); and

"(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

"(A) as a material weakness in reporting under section 3512 of title 31, United States Code; and

"(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Man-

agement Improvement Act (31 U.S.C. 3512 note).

''(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

''(A) the time periods, and

''(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

''(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

''(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

''§ 3535. Annual independent evaluation

''(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

''(2) Each evaluation by an agency under this section shall include—

''(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

''(B) an assessment (made on the basis of the results of the testing) of compliance with—

''(i) the requirements of this subchapter; and

''(ii) related information security policies, procedures, standards, and guidelines; and

''(C) separate presentations, as appropriate, regarding information security relating to national security systems.

''(b) Subject to subsection (c)—

''(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

''(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage

an independent external auditor to perform the evaluation.

''(c) For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

''(1) only by an entity designated by the agency head; and

''(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

''(d) The evaluation required by this section—

''(1) shall be performed in accordance with generally accepted government auditing standards; and

''(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

''(e) The results of an evaluation required by this section shall be submitted to the Director no later than March 1, 2003, and every March 1 thereafter.

''(f) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such

protections shall be commensurate with the risk and comply with all applicable laws and regulations.

''(g)(1) The Director shall summarize the results of the evaluations conducted under this section in a report to Congress.

''(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

''(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

''(h) The Comptroller General shall periodically evaluate and report to Congress on—

''(1) the adequacy and effectiveness of agency information security policies and practices; and

''(2) implementation of the requirements of this subchapter.

"§ 3536. Federal information security incident center

''(a) The Director shall cause to be established and operated a central Federal information security incident center to—

''(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

''(2) compile and analyze information about incidents that threaten information security;

''(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

''(4) consult with agencies or offices operating or exercising control of national security systems (including the National Security Agency) and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

''(b) Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

"§ 3537. National security systems

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of the information contained in such system;

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

''(3) complies with the requirements of this subchapter.

"§ 3538. Authorization of appropriations

''There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.''.

(2) CLERICAL AMENDMENT.—The items in the table of sections at the beginning of such chapter 35 under the heading ''SUBCHAPTER II'' are amended to read as follows:

''3531. Purposes.
''3532. Definitions.
''3533. Authority and functions of the Director.
''3534. Federal agency responsibilities.
''3535. Annual independent evaluation.

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3532(3) of title 44, United States Code.

(B) Section 2224 of title 10, United States Code, is amended—

(i) in subsection 2224(b), by striking ''(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)'' and inserting ''(b) OBJECTIVES OF THE PROGRAM.—'';

(ii) in subsection 2224(b), by striking ''(2) the program shall at a minimum meet the requirements of section 3534 and 3535 of title 44, United States Code.''; and

(iii) in subsection 2224(c), by inserting '', including through compliance with subtitle II

of chapter 35 of title 44'' after ''infrastructure''.

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this Act shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 2. MANAGEMENT OF INFORMATION TECHNOLOGY.

Section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) is amended to read as follows:

''SEC. 5131. RESPONSIBILITIES FOR FEDERAL INFORMATION SYSTEMS STANDARDS.

''(a)(1)(A) Except as provided under paragraph (3), the Director of the Office of Management and Budget shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) and in consultation with the Secretary of Commerce, promulgate standards and guidelines pertaining to Federal information systems.

''(B) Standards promulgated under subparagraph (A) shall include—

''(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

''(C) Standards described under subparagraph (B) shall be compulsory and binding.

''(D) The President may disapprove or modify such standards and guidelines if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Director shall immediately rescind or modify such standards or guidelines as directed by the President.

''(2) Standards and guidelines for national security systems, as defined under section 3532(3) of title 44, United States Code, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards—

''(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

''(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44, United States Code.

''(c) The promulgation of any standard or guideline by the Director under subsection (a), and the disapproval of any standard or guideline by the President under subsection (a)(1)(C), shall occur no later than 6 months after the submission of such standard or guideline to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).''.

SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), is amended by striking the text and inserting the following:

''(a) The Institute shall—

''(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

''(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3532(b)(2) of title 44, United States Code); and

''(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

''(b) The standards and guidelines required by subsection (a) shall include, at a minimum—

''(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agen-

cy based on the objectives of providing appropriate levels of information integrity, confidentiality, and availability according to a range of risk levels;

''(B) guidelines recommending the types of information and information systems to be included in each such category; and

''(C) minimum information security requirements for information and information systems in each such category;

''(2) a definition of and guidelines concerning detection and handling of information security incidents; and

''(3) guidelines for identifying an information system as a national security system.

''(c) In developing standards and guidelines required by subsection (a), the Institute shall—

''(1) consult with other agencies and offices (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, and the General Accounting Office) to assure—

''(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid

unnecessary and costly duplication of effort; and

''(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

''(2) submit to the Director of the Office of Management and Budget for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441)—

''(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section;

''(B) guidelines, as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this Act; and

''(C) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section; and

''(3) emphasize the development of policies and procedures that do not require specific technical solutions or products.

''(d)(1) There is established in the Institute an Office for Information Security Programs.

''(2) The Office for Information Security Programs shall be headed by a Director, who shall be a senior executive and shall be compensated at a level in the Senior Executive Service under section 5382 of title 5, United States Code, as determined by the Secretary of Commerce.

''(3) The Director of the Institute shall delegate to the Director of the Office of Information Security Programs the authority to administer all functions under this section, except that any such delegation shall not relieve the Director of the Institute of responsibility for the administration of such functions. The Director of the Office of Information Security Programs shall serve as principal adviser to the Director of the Institute on all functions under this section.

''(e) The Institute shall—

''(1) submit standards and guidelines developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

''(2) provide assistance to agencies regarding—

''(A) compliance with the standards and guidelines developed under subsection (a);

''(B) detecting and handling information security incidents; and

''(C) information security policies, procedures, and practices;

''(3) conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

''(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

''(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

''(6) solicit and consider the recommendations of the Information Security Advisory Board, established by section 21, regarding standards and guidelines that are being considered for submittal to the Director of the Office of Management and Budget in accordance with paragraph (1) and submit such recommendations to the Director of the Office of Man-

agement and Budget with such standards and guidelines submitted to the Director; and

''(7) report annually to the Director of the Office of Management and Budget on—

''(A) compliance with the requirements of this section, the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.), and other related requirements;

''(B) major deficiencies in Federal information security; and

''(C) recommendations to improve Federal information security.

''(f) As used in this section—

''(1) the term 'agency' has the same meaning as provided in section 3502(1) of title 44, United States Code;

''(2) the term 'information security' has the same meaning as provided in section 3532(1) of such title;

''(3) the term 'information system' has the same meaning as provided in section 3502(8) of such title;

''(4) the term 'information technology' has the same meaning as provided in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

''(5) the term 'national security system' has the same meaning as provided in section 3532(b)(2) of such title.

''(g) There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section.''.

SEC. 4. INFORMATION SECURITY ADVISORY BOARD.

Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4), is amended—

(1) in subsection (a), by striking ''Computer System Security and Privacy Advisory Board'' and inserting ''Information Security Advisory Board'';

(2) in subsection (a)(1), by striking ''computer or telecommunications'' and inserting ''information technology'';

(3) in subsection (a)(2)—

(A) by striking ''computer or telecommunications technology'' and inserting ''information technology''; and

(B) by striking ''computer or telecommunications equipment'' and inserting ''information technology'';

(4) in subsection (a)(3)—

(A) by striking ''computer systems'' and inserting ''information system''; and

(B) by striking ''computer systems security and privacy'' and inserting ''information security'';

(5) in subsection (b)(1) by striking ''computer systems security and privacy'' and inserting ''information security'';

(6) in subsection (b) by striking paragraph (2) and inserting the following:

''(2) to advise the Institute and the Director of the Office of Management and Budget on information security issues pertaining to Federal Government information systems, including through review of proposed standards and guidelines developed by the Director of the National Institute of Standards and Technology under section 20; and'';

(7) in subsection (b)(3) by inserting ''annually'' after ''report'';

(8) by inserting after subsection (e) the following new subsection:

''(f) The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.'';

(9) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively;

(10) by striking subsection (h), as redesignated by paragraph (9), and inserting the following:

''(h) As used in this section, the terms ''information system'' and ''information technology'' have the meanings given in section 20.''; and

(11) by inserting at the end the following:

''(i) There are authorized to be appropriated to the Secretary of Commerce $1,250,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the Information Security Advisory Board to identify emerging issues related to information security, and to convene public meetings on those subjects, receive presentations, and publish reports and recommendations for public distribution.''.

SEC. 5. TECHNICAL AND CONFORMING AMENDMENTS.

(a) COMPUTER SECURITY ACT.—Sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note) are repealed.

(b) FLOYD D. SPENCE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2001.—The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398) is amended by striking subtitle G of title X.

(c) PAPERWORK REDUCTION ACT.—(1) Section 3504(g) of title 44, United States Code, is amended—

(A) by adding ''and'' at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking ''sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)'' and inserting ''subchapter II of this title''; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

(2) Section 3506(g) of such title is amended—

(A) by adding ''and'' at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking ''the Computer Security Act of 1987 (40 U.S.C. 759 note)'' and inserting ''subchapter II of this title''; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

SEC. 6. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 30 days after the date of the enactment of this Act.

○